Statement of Jeffrey J. Danneels
Department Manager, Security Systems and Technology Center
Sandia National Laboratories

United States House of Representatives
Committee on Science
Hearing on H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure
November 14, 2001

INTRODUCTION

Chairman Boehlert and distinguished members of the committee, thank you for inviting me here today to testify on the topic of developing anti-terrorism tools for the water infrastructure. My name is Jeffrey J. Danneels and I lead the effort at Sandia National Laboratories (Sandia) to improve water infrastructure security. Sandia National Laboratories is managed and operated for the U.S. Department of Energy (DOE) by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation.

Sandia is a multiprogram laboratory of DOE and one of the three National Nuclear Security Administration laboratories with research and development responsibilities in nuclear weapons and associated programs in nonproliferation and arms control. As a multiprogram national laboratory, Sandia also supports security programs in energy, critical infrastructures, and emerging threats, as well as work for the DOE, the Department of Defense, and other federal agencies.

As the lead laboratory for physical security research and development for DOE's Office of Safeguards and Security, Sandia has a rich history providing security solutions for high-consequence facilities. Over the past 25 years, DOE has invested over $500 million in Sandia's security programs. The results of this investment include unique sensor-testing facilities, advanced security systems, a wealth of system-testing experience and capabilities, and a large, multidisciplinary technical base. Sandia's extensive security experience is complemented by a wide range of inhouse science and engineering expertise, including water resources management and use, advanced water treatment techniques, cooperative water agreement monitoring programs, and contaminant fate and transport, as well as dynamic simulation modeling. This expertise in related water areas complements and provides technical support to Sandia's work in water infrastructure security. Sandia also has many years of experience in the information security arena. Beginning with command and control for nuclear weapons, Sandia's expertise has expanded to include network security, cryptography, secure Supervisory Control and Data Acquisition (SCADA) for critical infrastructures, and information system security assessments.

This testimony presents a phased approach to improving the security of the water infrastructure. The immediate steps already undertaken to improve security, such as adding guards and additional water-testing protocols, are neither sustainable, nor do they provide a balanced approach for improving security in all parts of the water infrastructure. In parallel with the immediate response, research should begin on intermediate and long-term solutions that will significantly reduce the security risk to America's water infrastructure. As an example, real-time monitoring for chemical and biological contamination could become a reality in the next three to five years. In the long term, systems studies for understanding the most effective methods to meet new drinking water

quality standards while providing enhanced security may point to fundamental water system changes. Recommendations for a focused and effective research program to address these issues will be presented in the conclusion of this statement.

As the responsible public agency for the protection of the water infrastructure, the Environmental Protection Agency (EPA) joined with the American Water Works Association Research Foundation (AwwaRF) and Sandia to address the security issues surrounding our national water infrastructure. Sandia is presently developing a security risk assessment methodology for the water infrastructure. This methodology addresses security from a systems perspective by considering both physical and cyber security and their interdependencies with other critical infrastructures.

BACKGROUND

To improve the security of our nation's water infrastructure, the present conditions of the water infrastructure and needs for the future must first be understood. A snapshot of the current national water infrastructure can be drawn from the publications of the EPA, the American Water Works Association (AWWA), the AwwaRF, the National Research Council, the Water Infrastructure Network (WIN), and other water utility specialists. While many of the identified water infrastructure requirements do not directly relate to security, meeting these requirements provides ample opportunity to enhance security as improvements are implemented. Now is the time to ascertain whether fundamental changes in the way the water industry supplies drinking water can result in cost-effective improvements across the spectrum of current water infrastructure concerns.

Water Infrastructure

The EPA (1999) has explored the size and number of the water utilities that comprise our national water infrastructure. Approximately 170,000 public water systems provide water for more than 250 million Americans. Public water systems are "water systems that provide drinking water to at least 25 people or 15 service connections for at least 60 days per year." The EPA recognizes two primary types of public water systems:

- **Community Water Systems**, which provide drinking water to the same people year-round. Approximately 54,000 community water systems currently serve America's homes. Of these community water systems, about 350 are large enough to serve more than 100,000 customers.
- **Non-Community Water Systems**, which serve customers on less than a year-round basis. These systems can be further subdivided into two categories:
    1) Non-community water systems that serve 25 or more people for more than six but less than 12 months, such as schools or factories with their own water sources. America has more than 20,000 of these systems.
    2) Non-community water sources that provide water to sites where people are transient, such as gas stations or campgrounds. More than 96,000 systems fit this category (EPA, 1999).

Literature searches that cover the past 100 years reveal very few malevolent attacks on the water infrastructure in the United States. The information that is available is of limited use to predict the types of attacks that might be perpetrated in the coming years.

Outdated and Resource-Limited Infrastructure

There were more than 270 million water-consuming Americans at the turn of the new century, which included an increase of about nine percent during the 1990s for a total increase of 120 million (80 percent increase) since 1950. The U.S. Census Bureau's middle estimate projects another 120 million people added by 2050. "The implications of this forecast, even if not fully realized, are manifold and complex: the nation will essentially have to replicate all the housing and infrastructure built since World War II, in addition to repairing and replacing what already exists" (according to the National Research Council, 2001). The anticipated additional burdens upon the aging water infrastructure are a significant consideration. To meet the water needs of 390 million Americans in 2050, a clear strategy must be developed now. According to an AWWA report that analyzed 20 utilities, "expenditures on the order of $250 billion over 30 years might be required nationwide for the replacement of worn-out drinking water pipes and associated structures (valves, fittings, etc.). This figure does not include wastewater infrastructure or the cost of new drinking water standards" (AWWA, 2001).

The typical high-volume, urban domestic water utility was designed to deliver water for fire-fighting as well as for public consumption. In many cases, less than one percent of the treated water flowing from an urban water utility is consumed (drinking and cooking). In Milwaukee, for example, 41 billion gallons per year of treated water is pumped into the distribution pipeline. This amounts to over 125 gallons per user per day. Yet only about one-half gallon, or less than one-half percent of this volume, is consumed by the user each day. Similarly, Albuquerque pumped 38.6 billion gallons of well water to serve approximately 450,000 residents in 1999, which is over 235 gallons per user per day (City of Albuquerque, 2000). Less than one-quarter of one percent of the treated volume was consumed. Why is 100 percent of the water supply being protected at the same level as the one percent that poses the greatest health threat?

Natural outbreaks, such as *Cryptosporidium*, have already shown the risks in the current system for the immunity-compromised, the very young, and the aged populations. A survey of the literature documents only one death in the United States from intentionally contaminated water in the past 100 years (Tucker and Sands, 1999). However, doctors from Harvard and the Medical College of Wisconsin estimated that as many as 10,700 or more rectal and bladder cancers may be caused each year by trihalomethanes and other water disinfection byproducts (Morris et al., 1992). The Journal of Epidemiology also reports that these chemicals are associated with pancreatic cancer (Geldreich et al., undated) and may be associated with major birth defects (Bove et al., 1992). Historically, chemicals intentionally introduced into the water system for disinfection or other treatment processes posed more of a threat to the health of the general public than poisons emplaced by criminals or terrorists.

In April 2000 WIN released its first report, documenting the need for significant improvements in water quality and public health. These proposed improvements, although not universally accepted, were associated with America's investments in the water and wastewater infrastructures. This report also projected the financial costs of maintaining such a level of improvement. Between now and 2020, a $23 billion per year increased investment will be required to meet national environmental and public health priorities and to repair and replace the crumbling water infrastructure. WIN, representing professional, technical, academic, environmental, labor, and government organizations involved in water infrastructure, declared that new investments are needed in the amount of nearly a trillion dollars in critical water and wastewater improvements over the next two decades. "Not meeting the investment needs of the next 20 years risks reversing the public health, environmental, and economic gains of the last three decades" (WIN, 2001).

Although violations of the Safe Drinking Water Act regulations are on the decline, significant numbers of systems affecting tens of millions of customers are out of compliance for one or more of the EPA-regulated contaminants. In fact, the EPA has concluded that the number of monitoring and reporting violations is greatly underestimated:

> Over the past year, EPA has been evaluating the quality of the data used to assess the effectiveness of the drinking water program . . . . This analysis concluded that about 90 percent of monitoring and reporting violations which should have been reported were reported incorrectly or not at all (EPA, 1999).

Solutions are needed that address all these concerns. Enhanced security features for water utilities should become an important feature of all new designs and retrofits. In addition to the oft-mentioned chemical and biological contamination threats, water utility targets could include physical and cyber disruption of facilities resulting in long-term shortages or loss of public confidence.

WATER INFRASTRUCTURE SECURITY PROGRAM – PHASED APPROACH

The events of September 11, 2001, caused the nation to consider the vulnerability of many of our critical infrastructures. The water infrastructure was not built to withstand terrorism and is vulnerable to four broad classes of attacks:

- Chemical contamination,
- Biological contamination,
- Physical disruption, and
- Disruption of the computerized control network known as the SCADA system.

Improving security system effectiveness or reducing the consequences of an attack are the two most important ways to reduce water infrastructure risk. The ultimate goal of a water infrastructure security program is to make the water infrastructure an unattractive target for terrorism. The purpose of this testimony is to help identify an effective, phased approach for achieving this goal. The many forces driving change in the reliability and safety of the water infrastructure provide ample opportunities to improve security in parallel with other required modifications.

The water infrastructure is subject to a large number of additional needs and financial stresses beyond terrorist attack and other malevolent human threats:

- Monitoring and reporting requirements have increased significantly.
- There is a continuing need for investment in new facilities to keep pace with expected population growth.
- A large maintenance and upgrade investment is necessary to replace aging infrastructure.
- Additional financial investments will be required to address the large number of contaminants under consideration for regulation by the EPA as well as those contaminants yet to be studied or even identified.
- Many of the standards for regulated water contaminants are expected to become more stringent in the near future.

Water system managers are under enormous pressure to improve the security of the water supply in the coming weeks or months. Unfortunately, the realities of the existing infrastructure—unprotected reservoirs, systems with no water treatment capabilities, large and aging treatment facilities, open and broadly dispersed distribution systems, minimal real-time monitoring capabilities, under-protected information and SCADA systems, and the lack of ties between water delivery systems—render it extremely difficult to protect. There is no quick or cheap fix.

Phased Approach

A phased approach to improve water infrastructure security will yield the best results. The phases to reduce identified risks to the water supply infrastructure include the near term, which will yield results in the next one to three years; the intermediate term, which is three to five years from now; and the long term, from five to ten years in the future. Actions on all phases should begin immediately.

Near Term

There are four areas of security that should be addressed in the near-term phase: threat definition, information protection, short-term risk reduction, and training.

Threat definition: The range of threats that a water utility should be prepared to address must be better defined. Some government agencies have drafted what they believe is their credible threat spectrum or description into a classified document. These agencies want their protection systems for critical facilities to have a reasonable likelihood of stopping specific defined threats. Until the water industry understands and defines the probable threats to its systems, there can be no consistency across the infrastructure.

Engaging the Federal Bureau of Investigation, the Centers for Disease Control, and other information and intelligence agencies to help define the threat is an important near-term step. Defining the threat or threats against which the water infrastructure should be protected is the necessary first step in improving security. This threat can be graded based upon the severity of the consequences that threat-caused disruptions have on a specific water system; but without this consistent threat definition, the security requirements, preparedness, and capabilities of the water infrastructure and its individual systems cannot be assessed or compared.

Information protection: Because many drinking water utilities are operated or administered by local governments, they are subject to state disclosure laws, often referred to as sunshine laws. These state laws are not pre-empted by federal laws. Appropriate methods to protect security information and the results of vulnerability assessments at drinking water utilities must be implemented in the near term.

For example, the Association of Metropolitan Water Agencies received a grant from the EPA to create an Information Sharing and Analysis Center (ISAC). This badly needed tool will help disseminate security information and knowledge among drinking water utilities, but the ISAC information itself may be subject to sunshine law disclosure requirements once the information is accessed or used by a utility. Obviously, existing sunshine laws would severely limit the desirability of participating with ISAC or sharing the type of information that the ISAC could provide to other utilities. The Critical Infrastructure Protection Advisory Group, made up of water industry associations, government agencies, and several water utilities that represent the water sector, should address this issue and provide guidance to Congress for possible legislative changes.

Short-term risk reduction: A security risk assessment methodology for the water infrastructure is being developed and field-tested and will require several months to complete. Having a standard methodology for assessing the security risks in the water infrastructure will help ensure the completion of comprehensive and comparable risk assessments. Sandia is also performing security risk assessments of specific water utility systems in parallel with the methodology development. This effort will identify a spectrum of short-term improvements that can be quickly implemented either to increase protection system effectiveness or to

reduce consequences or potentially do both. However, this first-round effort cannot be as thorough as desired due to the lack of knowledge about potential chemical and biological contaminants as well as other credible threats.

Short-term security improvements include upgrades to physical and cyber security systems, developing security processes and procedures, implementing operational changes, increasing water quality testing protocols, and completing background checks on employees. Instrumentation presently in use to measure pH, chlorine residual, total organic carbon, conductivity, and other parameters may also be employed to detect impacts on water quality from malevolent acts.

Training: Developing and refining the security risk assessment methodology for water utilities and training the utility personnel and their consultants on the methodology are important near-term steps. AwwaRF and the EPA are partnering with Sandia to develop and present a three-day course on performing risk assessments for water systems in December of 2001. Although the methodology is not expected to be completely verified and validated by that time, the urgency of the need for this tool is immediate.

This course will include classroom training as well as a practical application that will enable the trainees to begin a risk assessment of their own facilities. EPA is also partnering with Sandia to develop a "Train the Assessor" course to train consultants to perform water system risk assessments and to evaluate the potential risk reduction from proposed operational and security upgrades. This training will provide hands-on experience with many physical protection technologies so that participants can understand their uses and limitations.

Awareness training can also improve water security. Industry associations are supplying awareness videos to their memberships, their websites are full of helpful information, and awareness courses are being planned. The goals of the awareness program are to educate water utility owners and operators on the importance of protecting the water infrastructure and to initiate steps to implement and accomplish this protection.

Intermediate Term

In the three-to-five-year range, water utilities should take a more balanced approach to the security of their systems. Installing real-time monitoring equipment, improving redundancy, adding back-up systems, enhancing SCADA security, and employing security technologies should be accomplished over the intermediate term. A balanced approach is necessary to ensure that the security of the entire system is enhanced; otherwise, weak links can be exploited by an adversary. All parts of the water infrastructure, including the supply, treatment, and distribution components, require improvements to achieve a consistent level of protection throughout the system.

Real-time monitoring: New monitoring capabilities to detect water-borne chemical and biological contaminants are needed throughout the water infrastructure, from source water monitoring to continuous monitoring at multiple locations throughout the distribution system. Monitoring the source water will provide an early warning detection capability that allows water utilities to close water intakes in response to a drop in water quality. Monitoring the distribution pipelines and storage reservoirs will provide continuous feedback on water quality to detect malevolent contamination, allowing parts of the distribution system to be isolated in the event of an attack. More research is required to identify the potential biological and chemical contaminants that pose the greatest or most likely risk to the water infrastructure. A prioritized list of contaminants should be developed to drive the development of real-time sensing capabilities for those contaminants that present the greatest security risk. In the

intermediate term, existing instrumentation can be integrated with new microanalytical systems to provide real-time monitoring for many contaminants.

Sandia and the DOE Chemical/Biological Nonproliferation Program have invested more than $11 million to design and prototype hand-held chemistry laboratories. This work draws upon Sandia's expertise in microsystem technology to miniaturize laboratory chemical analysis. This effort has resulted in the development of two hand-portable systems capable of rapid and sensitive analysis of chemical constituents and impurities – one for gases and the other for liquids. The focus to date of the liquid analysis system has been biowarfare agents (biotoxins). Experiments with the prototype liquid analysis system demonstrated complete analysis of toxins in less than 4 minutes. With an investment in research and development, real-time sensing systems to monitor water quality could be made widely available. Not all contaminants can be detected in the intermediate-term, but the ability to detect many potentially deadly agents could significantly reduce the risk to the water consumer.

Redundancy: Risk can be reduced significantly by increasing the redundancy in the water infrastructure. These improvements reduce consequences rather than enhance security. The security risk assessment methodology can be used to identify components within the water utility that can leave the system vulnerable to "single points of failure," an engineering term used to identify weaknesses that can cause the entire system to fail. Adding pipelines, storage tanks, or alternate energy sources may eliminate these vulnerabilities and improve operational capabilities as well.

Back-up systems and spares: The water infrastructure is highly dependent on the electrical power grid to pump and treat water. However, loss of power does not result in an immediate loss of water supply for most water utilities because the amount of water stored in large reservoirs can be used for temporary supply. As with redundancy, additional back-up capabilities will reduce consequences. Back-up generators that are designed and installed, or working with the local power supplier to provide equipment during an extended power outage, can reduce risk by reducing consequences.

Many of the existing pumps, valves, and other mechanical equipment are old, and replacement parts are no longer available. Manufacturing spares of some critical components and storing them away from the facilities could reduce consequences of a physical attack as well as the consequences of an equipment failure.

SCADA improvements: Many of the legacy SCADA systems were designed with little or no protection. Standards are being developed to include enhanced security measures. Both legacy systems and new systems should include these updated features.

Security technologies: Once the threat or threats are better defined, appropriate application of security technologies should be part of the intermediate-term security improvement program. Detection, assessment, and delay elements can be incorporated around critical assets to help defeat an adversary. The security elements employed should become part of an independent protection system, rather than a part of the SCADA system and thus a collateral responsibility for facility operators. Also, a single point of failure vulnerability is created by routing the security system through the SCADA system.

Long Term

Over the long term, the changes to our water infrastructure are likely to be profound. Solutions to the security risks inherent in our water system can best be addressed through fundamental

changes that require a re-evaluation of the functions, capabilities, and limitations of the water infrastructure. The need for revitalizing our deteriorating water infrastructure, the growing demand from increasing populations, and the anticipated more stringent water quality regulations combine with the emerging requirements for improved security to drive system owners and operators to consider fundamentally changing the way water is provided to users. Water sources will be difficult, if not impossible, to protect from intentional contamination. Huge water treatment plants covering acres of often-vulnerable real estate are too big to cost-effectively protect against intrusion. Water distribution pipelines have hundreds of thousands of access points. Traditional security measures such as increased physical security (e.g., guards and fences) can help, but these measures constitute neither a complete nor a very cost-effective solution. Fundamental changes in our approach to potable water supply, treatment, and delivery may be required to provide the most efficient and economical approach to water supply safety, security, and reliability. Researching alternative solutions, looking for ways to reduce the consequences of an attack or accident, developing advanced treatment technologies, moving toward distributed treatment, crafting new drinking water safety and security standards, understanding how to protect critical assets, and providing water system security education are long-term solutions to the problems faced by the water infrastructure.

Alternative solutions: A range of solutions can be considered. The solution alternatives that should be investigated for applicability and feasibility include use of bottled water, point-of-use or point-of-entry treatment, distributed treatment, and dedicated potable water distribution. On one end of the spectrum are the high-end advanced membrane filtration systems (reverse osmosis) coupled with granular activated carbon that might be employed at the water treatment facility to provide bottled water for an entire community. The expense of producing the water is almost insignificant compared to the costs of bottling and distributing the treated water, but the final cost is likely to be much lower than today's bottled water. On the other end of the spectrum would be small point-of-use treatment applications. Such systems as under-the-sink faucet filters, employing advanced membranes or other technologies, could be used to reduce biological as well as many of the chemical hazards. Filtration processes and some treatment activities at the water treatment facility would continue, but final drinking water quality treatment would be at the point-of-use or point-of-entry.

Reducing consequences: End-users want to be guaranteed that the water they are consuming is safe. Zero risk cannot be achieved, but new or retrofitted facilities and operations may provide a much greater probability of delivering safe water through our taps. The security risk assessment methodology applied to the water infrastructure elevates the importance of consumed (drinking and cooking) water because an attack affecting consumed water would have the highest likelihood of impacting large populations and hence have the greatest consequences. While more study is required to identify the toxicity of biological contamination through cutaneous contact with water, inhalation and ingestion routes of human exposure are now of highest concern.

Advanced treatment technologies: If the option is considered to protect the one percent of water that is consumed for drinking and cooking, the question then becomes how that goal is best achieved. Biological contamination has been singled out as a concern, both as a malevolent and a natural threat. Existing technologies of sand/anthracite filtration, micro- and ultrafiltration, and treatments with ozone, ultraviolet, and chlorine significantly reduce biological threats. Nanofiltration and reverse osmosis systems can filter out biological contaminants in the range of 0.001 microns and greater (Osmonics, Inc., 1996). Pathogenic biological organisms that fall into this size category include *Cryptosporidium*, *Giardia*, viruses, fecal

coliforms, and various bioagents such as anthrax spores. Many of the chemical contaminants that might be used to contaminate water supplies can also be removed using these advanced treatment technologies. These same technologies, particularly the advanced membranes, can be used to more effectively treat saline water as well. Treating only one percent of the water would allow us to use these sophisticated treatment technologies that are prohibitively expensive for use on all the water. Further research is needed to improve both the effectiveness of removing contaminants as well as the cost effectiveness of these methods.

Distributed treatment: The middle of the spectrum that ranges from point-of-use approaches to whole-system treatment solutions includes localized or community-based systems that provide the final drinking water quality treatment. These systems could serve hundreds of customers or individual buildings. The treatment systems would be very small if dedicated potable water distribution were included in this approach. Distributed systems would make it very difficult to attack a large population. This option seems to offer an attractive economy of scale compared to filtration units in every home or building a new delivery system for bottled water. Over the past five years, the EPA's Environmental Technology Verification (ETV) Program (EPA, 2001), in cooperation with the National Sanitation Foundation, has been verifying the performance of a variety of innovative (ultraviolet, filtration, ozonation) drinking water package treatment plants that could potentially be candidate regional/neighborhood treatment systems.

New drinking water safety and security standards: Solutions are needed that reduce risk to the public and offer the ability to meet the anticipated more stringent drinking water standards. The proposed arsenic standard is an example of a new regulation that will require significant investments in the water infrastructure, a treatment that is unnecessary for 99 percent of the water processed. Point-of-use, bottling water at the treatment facility, and neighborhood-finished treatment systems may offer a more economical solution to meeting new standards. Performing security risk assessments on the water infrastructure on a periodic schedule will help ensure that needed operational and security improvements are reducing risk.

Critical assets: With a fundamental change to the distribution system, it becomes much easier to determine the critical assets in the water infrastructure, such as pipelines and pumps. Many pipelines are deeply buried and thus are an unlikely target. However, main lines that are exposed may need increased security. If physical security measures can be employed to protect the existing pumps and new designs developed to separate and protect future pumps, the risk of physical disruption of the water supply can be significantly reduced. Another method to reduce water supply risk would be to tie major metropolitan water systems together. Most large metropolitan areas have the ability to treat and provide more water than is typically demanded by their customers. By constructing pipelines among the utilities and adding additional pumping capacity, the utilities would become more distributed, thus reducing the consequences of an outage.

Education: Finally, once a course of action is determined, future water system designers must be educated and trained in these methods. Security measures and features designed and constructed at the onset of a project will cost significantly less than trying to add these features later. The water community will need to reach out to the American Society of Civil Engineers (ASCE), the AWWA, colleges, and other institutions to educate future designers on the new requirements identified for water utilities. The ASCE and the AWWA already work together to set standards for drinking water utilities, a partnership that can be used to implement needed security upgrades.

CONCLUSIONS

Efforts underway, such as the development of the security risk assessment methodology for water utilities, will require investments in the water infrastructure to provide a solid foundation for improving security. Refining and automating the methodology are clearly necessary efforts. This methodology will require significant development as more information is gained about potential contaminants and other credible threats to the water infrastructure. A clear understanding of potential threats and agreement at the national level about their credibility is important. The water utility risk assessment is a snapshot in time and should be repeated on a periodic basis.

Throughout the water infrastructure, but especially in the source water and distribution systems, early warning monitoring capabilities must be developed and installed. "There is a critical need for rapid online and field methods for detecting and quantifying both infectious agents and biotoxins in water and in other environmental samples" (Burrows and Renner, 1999). "The need for and scope of an early warning monitoring system should be guided by an assessment and prioritization of site-specific risks that includes a vulnerability analysis of the entire water supply system, including the watershed and distribution system" (ILSI, 1999). We must know what is in the water and have time to react before it is consumed.

The current method by which water is treated and delivered should be re-evaluated. Distributed treatment systems, bottled water facilities at the water treatment plant, point-of-use filtration, or a combination of these measures will improve the security of consumed water. "The delegates to the American Assembly recommend utilities: Explore a new water deliver approach whereby water is treated to adequately protect against acute health risks. This approach could include additional polishing to protect against chronic risks for only that water used for actual human consumption" (Means, undated). More research is needed into methods to reduce the cost and improve the efficiency of treating saline water, which often relies on the same advanced technologies that new approaches to water delivery would employ. Treating 100 percent of the water to drinking quality while consuming less than one percent may no longer make sense. The socioeconomic consequences of all alternatives must be studied and understood.

A thorough study of the various alternatives and a cost/benefit analysis must be performed and a range of options developed for utilities to choose how best to improve their systems. The proposed alternatives all have advantages and disadvantages. Bottling water at the plant allows the equipment to be well maintained, uses the existing infrastructure, and employs economies of scale. Limitations include the challenges of developing a system to effectively deliver the water and gaining customer acceptance. Point-of-use systems provide the greatest security, but have many drawbacks. The sheer numbers of devices required, maintenance issues, and the amount of water passing through some systems and then sent into the wastewater system would need to be addressed. Public education and transferal of public health responsibility to the consumer might not be acceptable.

Education and training are critical to the overall success of this program. Future designers of water supply systems need to be educated to consider security at the beginning of the design process. Water supply system operators and their vendors need to understand and assess the potential security risks in their systems and develop ways to manage, mitigate, or otherwise reduce those risks. The public needs to be educated to help protect their water supply and to understand why water delivery methods may need to change. Our collective goal is to make the water infrastructure an unattractive target for terrorism.

RECOMMENDATIONS ON H.R. 3178

A research and development (R&D) program should be initiated immediately to study intermediate and long-term approaches to significantly reduce risk in the water infrastructure. Many of the efforts described in H.R. 3178 are the cornerstones of an effective R&D program. The work suggested by H.R. 3178 must be integrated with testing and other efforts underway to understand which contaminants are of the greatest risk to the water infrastructure.

H.R. 3178 should support the following efforts: the security risk assessment methodology for water systems, new security technologies, real-time monitoring, SCADA protection, and advanced treatment techniques.

The security risk assessment methodology will require significant improvement in the coming years both to reduce the cost of performing the assessments and to incorporate new features into the methodology. Some of the tools used in the methodology can be automated. The methodology must be flexible to incorporate new threat information as it becomes available and generic to cover a wide range of systems. The methodology as developed is designed for medium and large cities; a parallel effort is required to determine the best approach for small systems.

New security technologies are being developed for specific infrastructure threats, such as the explosives detection portal for airports. Security technologies that may be required for water utilities might include on-line radiation monitors to detect radiation contamination in large flows of water, active access delay systems for remotely controlled facilities, and remote response platforms.

A significant effort will be required to design, integrate, miniaturize, and cost-effectively produce a knowledge-based, real-time monitoring system. Many of the biological contaminants of concern are difficult to detect and require several days to complete the existing identification testing protocols utilizing expensive instrumentation. Much of the basic research on new identification schemes is scattered at numerous institutions around the country. A new model of cooperation may be required to develop integrated sensors into a real-time water quality monitoring capability. A systems integrator agency or organization should be responsible from the start for the effort to integrate, miniaturize, and produce a viable, cost-effective system.

The existing SCADA systems have many vulnerabilities, yet these computerized controls will play an increasingly important role as automation is employed to reduce operating costs. Both legacy systems and new systems are vulnerable to hackers. Standards, security and operational protocols, and secure platforms all require research and development to protect the control system.

Research into advanced treatment techniques to remove a broad range of potential contaminants both for protection from intentional acts and to meet new drinking water standards is necessary. This research will support the analysis to determine whether fundamental changes are needed in the way America's potable water is supplied. A parallel effort to understand the most cost-effective manner to supply reliably safe, secure water should be a top priority. This effort will provide the long-term solutions.

H.R. 3178 should provide flexibility in approaches and funding to support this type of effort. Current water programs to protect potable water may need to be extended or altered to meet the new enhanced security requirements. Integrating security while solving the other needs of the water infrastructure is the right approach.

Finally, H.R. 3178 provides accountability, focus, and structure for a security program within the water infrastructure.

REFERENCES

AWWA, 2001. *Dawn of the Replacement Era: Reinvesting in Drinking Water Infrastructure,* AWWA Water Industry Technical Action Fund study, American Water Works Association, Denver, CO, May 2001.

Bove, F. J., et al., 1992. *Public Drinking Water Contamination and Birthweight, Fetal Deaths, and Birth Defects* and *Public Drinking Water Contamination and Birthweight and Selected Birth Defects*, U.S. Public Health Service and the New Jersey Department of Health, 1992.

Burrows, W. Dickinson and Renner, Sara E., 1999. *Biological Warfare Agents as Threats to Potable Water* **in** Environmental Health Perspectives, v. 107, no. 12, pp.975-984, National Institutes of Health, Washington, DC, December 1999.

City of Albuquerque, 2000. *Water Quality Report*, Water Quality Program, Public Works Department, Albuquerque, NM, July 2000.

EPA, 2001. See the EPA's Environmental Technology Verification (ETV) Program home page at: www.epa.gov/etv

EPA, 1999. 25 Years of the Safe Drinking Water Act: History and Trends, United States Environmental Protection Agency, Office of Water (4606), EPA 816-R-99-007, Washington, DC, December 1999.

Geldreich, E., et al., undated. *Summary Report: Investigation of the Cabool, Missouri Outbreak For a Water Supply Connection*, U.S. Environmental Protection Agency, Washington, DC.

ILSI, 1999. *Early Warning Monitoring to Detect Hazardous Events in Water Supplies* (An ILSI Risk Science Institute Workshop Report), Thomas M Brosnan (ed.), ILSI Press, Washington, DC, December 1999.

Means III, Edward G., et al., undated. *How to Best Position Your Utility for the Future*, available through the American Water Works Association Research Foundation, 6666 W. Quincy Ave., Denver, CO.

Morris, R. D., et al. 1992. *Chlorination, Chlorination By-Products, and Cancer: A Meta-Analyses* **in** American Journal of Public Health, v. 82, no. 7, pp. 955-963, 1992.

National Research Council, 2001. Envisioning the Agenda for Water Resources Research in the Twenty-first Century, Water Science and Technology Board/Division on Earth and Life Studies, National Research Council, Washington, DC, National Academy Press, 2001.

Osmonics, Inc. 1996. *The Filtration Spectrum,* copyrighted chart, Osmonics, Inc., Minnetonka, MN, 1996.

Tucker, Jonathon B. and Sands, Amy, 1999. *An Unlikely Threat* **in** Bulletin of the Atomic Scientists, v. 55, no. 4, July/August 1999.

WIN, 2001. *Recommendations for Clean and Safe Water in the 21st Century,* Water Infrastructure Network,Water Infrastructure Network, 1816 Jefferson Place, NW, Washington D.C. 20036-2505.

WITNESS DISCLOSURE INFORMATION

Witness name: Jeffrey J. Danneels

Capacity in which appearing: Representative of a non-government entity

Name of entity being represented: Sandia National Laboratories (GOCO)

Position held: Manager, Civilian Surety Programs Department

Parent organization (managing contractor): Lockheed Martin Corporation

Federal contract: Management and operating contract between Sandia Corporation and U.S. Department of Energy, DE-AC04-94AL85000. FY2002 estimated cost: $1,580,187,000; negotiated fee: $16,300,000.

Curriculum vitae:

Jeffrey J. Danneels is a Department Manager within the Security Systems and Technology Center at Sandia National Laboratories, a post he has held since June 1999. He is responsible for Civilian Surety programs, which include Security of large federal dams, Architectural Surety® for buildings, security of high-voltage transmission systems, and water security. Mr. Danneels was program director for the international *Innovative Technologies for Disaster Mitigation* conference (Oct '99) in Washington, DC. This three-day Architectural Surety® conference provided a forum for experts from around the world to exchange information on mitigating the consequences of natural and man-made disasters.

Prior to this position, Mr. Danneels was the Las Vegas Operations Manager for the Yucca Mountain Project site characterization activities, which include the design and installation of experiments, numerical modeling, analyses of data, and formal reporting. His responsibilities included thermal testing, thermal-mechanical testing, convergence monitoring, and rock properties testing.

From 1994 to 1997, Mr. Danneels served as department manager for Sandia's Energy and Environment Sector Office Team. Responsibilities included developing and monitoring business metrics as well as representing Sandia's Energy and Environment business unit to sponsors and various other entities, including congressional staff, universities, and other national laboratories and institutions.

From 1989 to 1994, Mr. Danneels served as Sandia's department manager for the Facilities Accelerated System Team, which was responsible for developing and deploying a process to rapidly install complex equipment in ultra-clean-room environments. He was the responsible manager for construction projects that include Sandia's Explosives Components Facility, Strategic Defenses Facility, and Technology Development Center. In this capacity, Mr. Danneels pioneered innovative performance-based contracts to greatly shorten the Architectural/Engineering firm selection process for line-item projects.

Mr. Danneels joined Sandia in 1985. He holds a Masters of Management from the University of New Mexico, a Masters of Science in Civil Engineering from Louisiana State University, and a Bachelor of Science in Civil Engineering from Michigan State University.

Mr. Danneels has received several significant honors for his work at Sandia, including three Sandia President's Quality Awards and, most notably, an Employee Recognition Award in 1998 for the early completion of the installation phase of the Drift Scale Test on the Yucca Mountain Project, the largest in-situ rock thermal test in the world. The success of this project was noted by the chairman of the Nuclear Regulatory Commission in a letter to the United States Congress.